

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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 true. If  $\gcd(a, bc) = 1$ , then  $a$  doesn't share any prime factors with  $bc$ . Since the prime factors of  $b$  are a subset of these, they also can't overlap with the prime factors of  $a$ . Similarly for  $c$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1568, 546)$ . Show your work.

**Solution:**

$$1568 - 546 \times 2 = 1568 - 1092 = 476$$

$$546 - 476 = 70$$

$$476 - 70 \times 6 = 476 - 420 = 56$$

$$70 - 56 = 14$$

$$56 - 14 \times 3 = 0$$

So the GCD is 14.

3. (4 points) Check the (single) box that best characterizes each item.

For any positive integers  $p$  and  $q$ ,

if  $\text{lcm}(p, q) = pq$ , then  $p$  and  $q$  are relatively prime.      true       false

Zero is a factor of 7.

true       false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $c$ ,  $\gcd(ca, cb) = c \cdot \gcd(a, b)$

**Solution:** This is true.

$c$  divides both  $ca$  and  $cb$ . So  $\gcd(ca, cb)$  must have the form  $cm$ , where  $m$  is an integer. But then  $cm$  is the largest integer that divides both  $ca$  and  $cb$  if and only if  $m$  is the largest integer that divides both  $a$  and  $b$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2015, 837)$ . Show your work.

**Solution:**

$$2015 - 837 \times 2 = 2015 - 1674 = 341$$

$$837 - 341 \times 2 = 837 - 682 = 155$$

$$341 - 155 \times 2 = 341 - 310 = 31$$

$$155 - 31 \times 5 = 0$$

So the GCD is 31.

3. (4 points) Check the (single) box that best characterizes each item.

$\gcd(0, 0)$

0

k

undefined

$25 \equiv 4 \pmod{7}$

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (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 integer  $k$ ,  $(k - 1)^2 \equiv 1 \pmod{k}$ .

**Solution:** This is true. Notice that  $(k - 1) - (-1) = k$ . So  $k - 1 \equiv (-1) \pmod{k}$ . Therefore  $(k - 1)^2 \equiv (-1)^2 \equiv 1 \pmod{k}$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1183, 351)$ . Show your work.

**Solution:**

$$1183 - 3 \times 351 = 1183 - 1053 = 130$$

$$351 - 2 \times 130 = 351 - 260 = 91$$

$$130 - 91 = 39$$

$$91 - 3 \times 39 = 91 - 78 = 13$$

$$39 - 3 \times 13 = 0$$

So the GCD is 13.

3. (4 points) Check the (single) box that best characterizes each item.

If  $a$  and  $b$  are positive and  $r = \text{remainder}(a, b)$ ,  
then  $\gcd(b, r) = \gcd(b, a)$

true

false

$7 \mid -7$

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $\gcd(a, b) = 1$  and  $\gcd(b, c) = 1$ , then  $\gcd(a, c) = 1$ .

**Solution:** This is false. Consider  $a = c = 3$  and  $b = 2$ . Then  $a$  and  $b$  have no common factors, i.e.  $\gcd(a, b) = 1$ . Also  $b$  and  $c$  have no common factors, i.e.  $\gcd(b, c) = 1$ . But  $\gcd(a, c) = 3$ .

2. (6 points) Write pseudocode (iterative or recursive) for a function  $\text{gcd}(a,b)$  that implements the Euclidean algorithm. Assume both inputs are positive.

**Solution:**

$\text{gcd}(a,b)$

```

x=a
y=b
while (b > 0)
    r = remainder(a,b)
    a = b
    b = r
return a

```

3. (4 points) Check the (single) box that best characterizes each item.

$$\gcd(p, q) = \frac{pq}{\text{lcm}(p, q)}$$

( $p$  and  $q$  positive integers)      always            sometimes            never     

$-7 \equiv 13 \pmod{6}$       true            false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (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  $a$ ,  $b$ , and  $c$ , if  $a \mid bc$ , then  $a \mid b$  or  $a \mid c$

**Solution:** This is false. Consider  $a = 6$ ,  $b = 3$ ,  $c = 2$ . Then  $a \mid bc$ , but  $a$  doesn't divide either  $b$  or  $c$ .

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 the GCD is 37.

3. (4 points) Check the (single) box that best characterizes each item.

If  $a$  and  $b$  are positive integers

and  $r = \text{remainder}(a, b)$ ,

then  $\gcd(b, r) = \gcd(r, a)$

true

false

$$29 \equiv 2 \pmod{9}$$

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $\gcd(a, b) = n$  and  $\gcd(a, c) = p$ , then  $\gcd(a, bc) = np$ .

**Solution:** This is false. Consider  $a = b = c = 3$ . Then if  $\gcd(a, b) = 3$  and  $\gcd(a, c) = 3$ , but  $\gcd(a, bc)$  is 3, not 9.

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2380, 391)$ . Show your work.

**Solution:**

$$2380 - 391 \times 6 = 2380 - 2346 = 34$$

$$391 - 34 \times 11 = 391 - 374 = 17$$

$$34 - 17 \times 2 = 0$$

So the GCD is 17.

3. (4 points) Check the (single) box that best characterizes each item.

For any positive integers  $p$ ,  $q$ , and  $k$ ,  
if  $p \equiv q \pmod{k}$ , then  $p^2 \equiv q^2 \pmod{k}$

true

false

$2 \mid -4$

true

false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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 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!

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(7917, 357)$ . Show your work.

**Solution:**

$$7917 - 22 \times 357 = 63$$

$$357 - 5 \times 63 = 42$$

$$63 - 42 = 21$$

$$42 - 2 \times 21 = 0$$

So the GCD is 21.

3. (4 points) Check the (single) box that best characterizes each item.

If  $a$  and  $b$  are positive integers

and  $r = \text{remainder}(a, b)$ ,

then  $\gcd(a, b) = \gcd(r, a)$

true

false

$-2 \equiv 2 \pmod{4}$

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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

There is an integer  $n$  such that  $n \equiv 5 \pmod{6}$  and  $n \equiv 6 \pmod{7}$ ?

**Solution:** This is true. Consider  $n = 41$ .  $41 \equiv 5 \pmod{6}$  and  $41 \equiv 6 \pmod{7}$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1224, 850)$ . Show your work.

**Solution:**

$$1224 - 850 = 374$$

$$850 - 374 \times 2 = 850 - 748 = 102$$

$$374 - 102 \times 3 = 374 - 306 = 68$$

$$102 - 68 = 34$$

$$68 - 34 \times 2 = 0$$

So the GCD is 34.

3. (4 points) Check the (single) box that best characterizes each item.

Two positive integers  $p$  and  $q$  are relatively prime if and only if  $\gcd(p, q) = 1$ .

true

false

$0 \mid 0$

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_ Lecture: B

Discussion: Friday 11 12 1 2 3 4 5

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  $\gcd(a, c) = 1$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1012, 299)$ . Show your work.

$$1012 - 3 \times 299 = 1012 - 897 = 115$$

$$299 - 2 \times 115 = 299 - 230 = 69$$

$$115 - 69 = 46$$

$$69 - 46 = 23$$

$$46 - 2 \times 23 = 0$$

So the GCD is 23.

3. (4 points) Check the (single) box that best characterizes each item.

$$7 \mid 0$$

true  false 

$$k \equiv -k \pmod{k}$$

always  sometimes  never

Name: \_\_\_\_\_

NetID: \_\_\_\_\_ Lecture: B

Discussion: Friday 11 12 1 2 3 4 5

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  $a \neq b$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2737, 2040)$ . Show your work.

**Solution:**

$$2737 - 2040 = 697$$

$$2040 - 697 \times 2 = 2040 - 1394 = 646$$

$$697 - 646 = 51$$

$$646 - 51 \times 12 = 646 - 612 = 34$$

$$51 - 34 = 17$$

$$34 - 17 = 0$$

So the GCD is 17.

3. (4 points) Check the (single) box that best characterizes each item.

$$29 \equiv 2 \pmod{9}$$

true  false

Two positive integers  $p$  and  $q$  are relatively prime if and only if  $\gcd(p, q) > 1$ .

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_ Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (5 points) Let  $a$  and  $b$  be integers,  $b > 0$ . The formula  $a = bq + r$  partially defines the quotient  $q$  and the remainder  $r$  of  $a$  divided by  $b$ . What other constraint must we add to completely determine  $q$  and  $r$ ?

**Solution:**  $0 \leq r < b$

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2262, 546)$ . Show your work.

**Solution:**

$$2262 - 546 \times 4 = 2262 - 2184 = 78$$

$$546 - 7 \times 78 = 0$$

So the GCD is 78.

3. (4 points) Check the (single) box that best characterizes each item.

$$7 \mid 0$$

true  false

$$7 \equiv -7 \pmod{k}$$

always  sometimes  never

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $\gcd(a, b) > 1$  or  $\gcd(a, c) > 1$ .

**Solution:** This is true. If  $\gcd(a, bc) > 1$ , then there is some prime  $p > 1$  that divides both  $a$  and  $bc$ . Since  $p$  is prime,  $p$  must divide  $a$  or  $b$ . So  $\gcd(a, b) > 1$  or  $\gcd(a, c) > 1$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2079, 759)$ . Show your work.

**Solution:**

$$2079 - 759 \times 2 = 2079 - 1518 = 561$$

$$759 - 561 = 198$$

$$561 - 198 \times 2 = 561 - 396 = 165$$

$$198 - 165 = 33$$

$$165 - 33 \times 5 = 0$$

So the GCD is 33.

3. (4 points) Check the (single) box that best characterizes each item.

$$-2 \equiv 2 \pmod{9}$$
      true       false

If  $a$  and  $b$  are positive and  $r = \text{remainder}(a, b)$ ,  
then  $\gcd(b, r) = \gcd(b, a)$

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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 natural numbers  $a$  and  $b$ , if  $a \mid b$  and  $b \mid a$ , then  $a = b$ .

**Solution:** This is true. If  $a \mid b$  and  $b \mid a$ , then  $b = pa$  and  $a = qb$ , where  $p$  and  $q$  are integers. Since  $a$  and  $b$  are natural numbers and therefore not negative,  $p$  and  $q$  cannot be negative. So  $b = pqb$ , so  $pq = 1$ . So  $p = q = 1$  and therefore  $a = b$ . [This is more detail than you'd need for full credit.]

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2385, 636)$ . Show your work.

**Solution:**

$$2385 - 3 \times 636 = 2385 - 1908 = 477$$

$$636 - 477 = 159$$

$$477 - 3 \times 159 = 0$$

So the GCD is 159.

3. (4 points) Check the (single) box that best characterizes each item.

$-7 \equiv 13 \pmod{5}$       true       false

For any integers  $p$  and  $q$ , if  $p \mid q$  then  $p \leq q$ .      true       false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (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:** This is false.

Informally, since  $q$  is larger than  $p$ , congruence mod  $q$  makes finer distinctions among numbers than  $p$  does.

More formally, consider  $s = 1$ ,  $t = 4$ ,  $p = 3$  and  $q = 6$ . Then  $3 \mid 6$  and  $s$  and  $t$  are congruent mod 3, but  $s$  and  $t$  aren't congruent mod 6.

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(221, 1224)$ . Show your work.

**Solution:**

$$1224 - 5 \times 221 = 1224 - 1105 = 119$$

$$221 - 119 = 102$$

$$119 - 102 = 17$$

$$102 - 17 \times 6 = 0$$

So the GCD is 17.

3. (4 points) Check the (single) box that best characterizes each item.

$-7 \mid 0$       true       false

$k \equiv -k \pmod{7}$       always       sometimes       never

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (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  $a$ ,  $b$ , and  $c$ , if  $a \mid c$  and  $b \mid c$ , then  $ab \mid c$

**Solution:** This is not true. Consider  $a = b = c = 5$ . Then  $a \mid c$  and  $b \mid c$ . But  $ab = 25$  and  $c = 5$ . So  $ab$  does not divide  $c$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(7839, 1474)$ . Show your work.

**Solution:**

$$7839 - 5 \times 1474 = 7839 - 7370 = 469$$

$$1474 - 3 \times 469 = 1474 - 1407 = 67$$

$$469 - 7 \times 67 = 0$$

So the GCD is 67.

3. (4 points) Check the (single) box that best characterizes each item.

$-11 \equiv 4 \pmod{7}$       true       false

For any positive integers  $p$ ,  $q$ , and  $k$ ,  
if  $p \equiv q \pmod{k}$ , then  $p^2 \equiv q^2 \pmod{k}$       true       false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (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  $s \equiv t \pmod{q}$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(4340, 1155)$ . Show your work.

**Solution:**

$$4340 - 1155 \times 3 = 4340 - 3465 = 875$$

$$1155 - 875 = 280$$

$$875 - 280 \times 3 = 875 - 840 = 35$$

$$280 - 35 \times 8 = 0$$

So the GCD is 35.

3. (4 points) Check the (single) box that best characterizes each item.

$-7 \equiv 13 \pmod{5}$       true       false

$\gcd(k, 0)$  for  $k$  positive      0       k       undefined

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $a \neq b$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2015, 837)$ . Show your work.

**Solution:**

$$2015 - 837 \times 2 = 2015 - 1674 = 341$$

$$837 - 341 \times 2 = 837 - 682 = 155$$

$$341 - 155 \times 2 = 341 - 310 = 31$$

$$155 - 31 \times 5 = 0$$

So the GCD is 31.

3. (4 points) Check the (single) box that best characterizes each item.

$0 \mid 0$

true

false

Two positive integers  $p$  and  $q$  are relatively prime if and only if  $\gcd(p, q) > 1$ .

true

false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $\gcd(a, b) = n$  and  $\gcd(a, c) = p$ , then  $\gcd(a, bc) = np$ .

**Solution:** This is false. Consider  $a = b = c = 3$ . Then if  $\gcd(a, b) = 3$  and  $\gcd(a, c) = 3$ , but  $\gcd(a, bc)$  is 3, not 9.

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1609, 563)$ . Show your work.

**Solution:**

$$1609 - 2 \times 563 = 1609 - 1126 = 483$$

$$563 - 483 = 80$$

$$483 - 6 \times 80 = 3$$

$$80 - 26 \times 3 = 80 - 78 = 2$$

$$3 - 2 = 1$$

$$2 - 2 \times 1 = 0$$

So the GCD is 1.

3. (4 points) Check the (single) box that best characterizes each item.

For any positive integers  $p$  and  $q$ ,  
if  $\text{lcm}(p, q) = pq$ , then  $p$  and  $q$  are relatively prime.      true       false

$(5 \times 5) \equiv 1 \pmod{6}$       true       false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

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  $c$ ,  $\gcd(ca, cb) = c \cdot \gcd(a, b)$

**Solution:** This is true.

$c$  divides both  $ca$  and  $cb$ . So  $\gcd(ca, cb)$  must have the form  $cm$ , where  $m$  is an integer. But then  $cm$  is the largest integer that divides both  $ca$  and  $cb$  if and only if  $m$  is the largest integer that divides both  $a$  and  $b$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2380, 391)$ . Show your work.

**Solution:**

$$2380 - 391 \times 6 = 2380 - 2346 = 34$$

$$391 - 34 \times 11 = 391 - 374 = 17$$

$$34 - 17 \times 2 = 0$$

So the GCD is 17.

3. (4 points) Check the (single) box that best characterizes each item.

$25 \equiv 4 \pmod{7}$       true       false

Two positive integers  $p$  and  $q$  are relatively prime if and only if  $\gcd(p, q) = 1$ .      true       false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (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  $a$ ,  $b$ , and  $c$ , if  $a \mid bc$ , then  $a \mid b$  or  $a \mid c$

**Solution:** This is false. Consider  $a = 6$ ,  $b = 3$ ,  $c = 2$ . Then  $a \mid bc$ , but  $a$  doesn't divide either  $b$  or  $c$ .

2. (6 points) Write pseudocode (iterative or recursive) for a function  $\text{gcd}(a,b)$  that implements the Euclidean algorithm. Assume both inputs are positive.

**Solution:**

$\text{gcd}(a,b)$

```

x=a
y=b
while ( $b > 0$ )
    r = remainder(a,b)
    a = b
    b = r
return a

```

3. (4 points) Check the (single) box that best characterizes each item.

$2 \mid -4$

true

false

If  $a$  and  $b$  are positive and  
 $r = \text{remainder}(a, b)$ ,  
then  $\text{gcd}(a, b) = \text{gcd}(r, a)$

true

false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (5 points) Explain how to use the Euclidean algorithm to test whether two positive integers  $p$  and  $q$  are relatively prime.

**Solution:** Use the Euclidean algorithm to compute  $\gcd(p, q)$ . If the output is 1,  $p$ , and  $q$  are relatively prime.

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

**Solution:**  $1702 - 1221 = 481$

$$1221 - 481 \times 2 = 1221 - 962 = 259$$

$$481 - 259 = 222$$

$$259 - 222 = 37$$

$$222 - 6 \times 37 = 0$$

$$\text{So } \gcd(1702, 1221) = 37$$

3. (4 points) Check the (single) box that best characterizes each item.

If  $p$ ,  $q$ , and  $k$  are primes,  
then  $\gcd(pq, qk) =$

$q$       $pq$       $pqk$       $q \gcd(p, k)$

$$29 \equiv 2 \pmod{9}$$

true     false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 9 10 11 12 1 2 3 4 5 6

1. (5 points) For any real numbers  $x$  and  $y$ , let's define the operation  $\oslash$  by the equation  $x \oslash y = x^2 + y^2$ . Is the following claim true? Informally explain why it is, or give a concrete counter-example showing that it is not.

Claim: For any real numbers  $x, y$ , and  $z$ ,  $(x \oslash y) \oslash z = x \oslash (y \oslash z)$

**Solution:** This is not true. Consider  $x = y = 1$  and  $z = 2$ . Then  $(x \oslash y) \oslash z = (x^2 + y^2)^2 + z^2 = (1+1)^2 + 2^2 = 8$ . But  $x \oslash (y \oslash z) = x^2 + (y^2 + z^2)^2 = 1^2 + (1^2 + 2^2)^2 = 1 + 5^2 = 26$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(2737, 2040)$ . Show your work.

**Solution:**

$$2737 - 2040 = 697$$

$$2040 - 697 \times 2 = 2040 - 1394 = 646$$

$$697 - 646 = 51$$

$$646 - 51 \times 12 = 646 - 612 = 34$$

$$51 - 34 = 17$$

$$34 - 17 = 0$$

So the GCD is 17.

3. (4 points) Check the (single) box that best characterizes each item.

$$\gcd(p, q) = \frac{pq}{\text{lcm}(p, q)}$$

( $p$  and  $q$  positive integers)      always            sometimes            never     

$$-3 \equiv 3 \pmod{4}$$

true            false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 10 11 12 1 2 3 4 5 6

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

For any real numbers  $x$  and  $y$ , if  $x$  or  $y$  is irrational, then  $xy$  is irrational.

**Solution:** This is not true. Consider  $x = y = \sqrt{2}$ . Then  $x$  or  $y$  is irrational (because they are both irrational). But  $xy = 2$  which is rational.

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1012, 299)$ . Show your work.

**Solution:**  $1012 - 3 \times 299 = 1012 - 897 = 115$

$$299 - 2 \times 115 = 299 - 230 = 69$$

$$115 - 69 = 46$$

$$69 - 46 = 23$$

$$46 - 2 \times 23 = 0$$

So  $\gcd(1012, 299) = 23$

3. (4 points) Check the (single) box that best characterizes each item.

$$7 \mid -7$$

true  false

$$k \equiv -k \pmod{k}$$

always  sometimes  never

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 10 11 12 1 2 3 4 5 6

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  $\gcd(a, b) = 1$  and  $\gcd(b, c) = 1$ , then  $\gcd(a, c) = 1$ .

**Solution:** This is false. Consider  $a = c = 3$  and  $b = 2$ . Then  $a$  and  $b$  have no common factors, i.e.  $\gcd(a, b) = 1$ . Also  $b$  and  $c$  have no common factors, i.e.  $\gcd(b, c) = 1$ . But  $\gcd(a, c) = 3$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(3927, 637)$ . Show your work.

**Solution:**

$$3927 - 6 \times 637 = 3927 - 3822 = 105$$

$$637 - 6 \times 105 = 7$$

$$105 - 15 \times 7 = 0$$

So the GCD is 7.

3. (4 points) Check the (single) box that best characterizes each item.

$\gcd(k, 0)$  for  $k$       0            k            undefined     

$7 \equiv 5 \pmod{1}$       true            false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 10 11 12 1 2 3 4 5 6

1. (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:**  $0 \leq r < b$

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(4263, 667)$ . Show your work.

**Solution:**

$$4263 - 6 \times 667 = 261$$

$$667 - 2 \times 261 = 145$$

$$261 - 145 = 116$$

$$145 - 116 = 29$$

$$116 - 4 \times 29 = 0$$

So the GCD is 29.

3. (4 points) Check the (single) box that best characterizes each item.

For all prime numbers  $p$ , there are exactly  
two natural numbers  $q$  such that  $q | p$ .

true

false

Zero is a factor of 7.

true

false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 10 11 12 1 2 3 4 5 6

1. (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  $a$ ,  $b$ ,  $q$  and  $r$ , if  $a = bq + r$ , then  $\gcd(a, b) = \gcd(a, r)$ .

**Solution:** This is false. Consider  $a = 18$ ,  $b = 5$ ,  $q = 3$ , and  $r = 3$ . Then we have  $18 = 5 \cdot 3 + 3$ .  $\gcd(a, b) = 1$ , but  $\gcd(a, r) = 3$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1568, 546)$ . Show your work.

**Solution:**

$$1568 - 546 \times 2 = 1568 - 1092 = 476$$

$$546 - 476 = 70$$

$$476 - 70 \times 6 = 476 - 420 = 56$$

$$70 - 56 = 14$$

$$56 - 14 \times 3 = 0$$

So the GCD is 14.

3. (4 points) Check the (single) box that best characterizes each item.

If  $a$  and  $b$  are positive and  $r = \text{remainder}(a, b)$ ,  
then  $\gcd(b, r) = \gcd(b, a)$       true       false

$-7 \equiv 13 \pmod{6}$       true       false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 10 11 12 1 2 3 4 5 6

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

There is an integer  $n$  such that  $n \equiv 5 \pmod{6}$  and  $n \equiv 2 \pmod{10}$ ?

**Solution:** There is no such  $n$ . If  $n \equiv 5 \pmod{6}$  and  $n \equiv 2 \pmod{10}$ , then  $n = 5 + 6k$  and  $n = 2 + 10j$ , where  $k$  and  $j$  are integers. So  $5 + 6k = 2 + 10j$ . This implies that  $3 = 10j - 6k$  which is impossible because the right side is divisible by 2 and the left side isn't.

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(7917, 357)$ . Show your work.

**Solution:**

$$7917 - 22 \times 357 = 63$$

$$357 - 5 \times 63 = 42$$

$$63 - 42 = 21$$

$$42 - 2 \times 21 = 0$$

So the GCD is 21.

3. (4 points) Check the (single) box that best characterizes each item.

$$\gcd(0, 0)$$

0

k

undefined

$$29 \equiv 2 \pmod{9}$$

true  false

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

Lecture: A B

Discussion: Thursday Friday 10 11 12 1 2 3 4 5 6

1. (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 integer  $k$ ,  $(k - 1)^2 \equiv 1 \pmod{k}$ .

**Solution:** This is true. Notice that  $(k - 1) - (-1) = k$ . So  $k - 1 \equiv (-1) \pmod{k}$ . Therefore  $(k - 1)^2 \equiv (-1)^2 \equiv 1 \pmod{k}$ .

2. (6 points) Use the Euclidean algorithm to compute  $\gcd(1183, 351)$ . Show your work.

**Solution:**

$$1183 - 3 \times 351 = 1183 - 1053 = 130$$

$$351 - 2 \times 130 = 351 - 260 = 91$$

$$130 - 91 = 39$$

$$91 - 3 \times 39 = 91 - 78 = 13$$

$$39 - 3 \times 13 = 0$$

So the GCD is 13.

3. (4 points) Check the (single) box that best characterizes each item.

$$k \equiv -k \pmod{7}$$

always  sometimes  never

$$-2 \equiv 2 \pmod{4}$$

true  false