Amherst College
Department of Mathematics and Statistics

Math 250 — Midterm 1 Practice — 28 February 2025

Name: Solutions

Read This First!

- The exam uses **both sides of the page**.
- Keep cell phones off and out of sight.
- Do not talk during the exam.
- You are allowed one page of notes, front and back. No other books, notes, calculators, cell phones, communication devices of any sort, webpages, or other aids are permitted.
- Show **ALL** work clearly in the space provided or on the blank pages.
- In order to receive full credit on a problem, solution methods must be complete, logical and understandable.
- You may cite any theorems proved in class or on the homework in your proofs, except in cases where the statement to be proved is essentially the same as a theorem proved earlier. In that case you should write out the full proof. Please ask me if you are uncertain about whether you should prove a theorem or if it is enough to cite it.

Grading - For Instructor Use Only

Question:	1	2	3	4	5	6	$\sum$
Points:	12	12	12	12	12	12	72
Score:							

1. [12 points] Find all prime numbers p between 1 and 100 such that

$$p \equiv -1 \pmod{15}.$$

The integers in [1,100] congruent to -1 mod 15 are:

$$-1+15 = 14 = 2\cdot 7$$
$$14+15 = 29$$
$$29+15 = 44 = 2^2\cdot 11$$
$$44+15 = 59$$
$$59+15 = 74 = 2\cdot 37$$
$$74+15 = 89$$

We can check these individually to see that 29, 59, 89 are the primes in this list. We could also do the Sieve of Eratosthenes up to 100 & just check each number on the list.

2. [12 points] Recall that a *primitive Pythagorean triple* consists of three positive integers (a, b, c) such that

- $a^2 + b^2 = c^2$, and
- there are no common factors of a, b and c.

Find a primitive Pythagorean triple such that $a = 15$.

As we've seen in class, a PPT w/ a odd can be found by choosing two odd integers s,t w/ $s<t$ & no common factors, and choosing

$a = st$
$b = \frac{1}{2}(t^2 - s^2)$
$c = \frac{1}{2}(t^2 + s^2)$.

The derivation, if we forget:
$a^2 = c^2 - b^2$
$= (c+b)(c-b)$
Let $c+b = t^2$ & $c-b = s^2$,
so $a = st$, $b = \frac{t^2 - s^2}{2}$, $c = \frac{t^2+s^2}{2}$.

So to get $a=15$, we have two options:

option 1 $s = 3$, $t = 5$

$\Rightarrow$ $a = 15$
$b = \frac{1}{2}(25-9) = 8$
$c = \frac{1}{2}(25+9) = 17$
$\boxed{(15, 8, 17)}$

option 2 $s = 1$ $t = 15$

$\Rightarrow$ $a = 15$
$b = \frac{1}{2}(15^2 - 1^2) = \frac{1}{2} \cdot 224$
$= 112$
$c = \frac{1}{2}(15^2 + 1^2) = \frac{1}{2} \cdot 226$
$= 113$
$\boxed{(15, 112, 113)}$

3. [12 points] Compute the greatest common divisor of 1106 and 203.

Euclidean algorithm:

$r_{-1} = 1106$

$r_0 = 203$

$r_1 = 1106 \bmod 203$
$= 1106 - 5 \cdot 203 = 1106 - 1015$
$= 91$

$r_2 = 203 \bmod 91$
$= 203 - 2 \cdot 91 = 203 - 182$
$= 21$

$r_3 = 91 \bmod 21$
$= 91 - 4 \cdot 21 = 91 - 84$
$= 7$

$r_4 = 21 \bmod 7$
$= 21 - 3 \cdot 7$
$= 0.$

So $\gcd(1106, 203) = \gcd(7, 0)$
$= \boxed{7}.$

4. [12 points] Solve the following congruence.

$$28x \equiv 3 \pmod{149}$$

Check for common factors &/or find inverse w/ extended euclidean algorithm. In our shorthand:

$149u+28v$	u	v
149	1	0
$-5 \cdot 28$	$-5 \cdot 0$	$-5 \cdot 1$
$149-5\cdot 28 = -3 \cdot 9$	$-3 \cdot 1$	$-3(-5)$
$28 - 3\cdot 9 = 1$	-3	16

so $1 = -3 \cdot 149 + 16 \cdot 28$

$\Rightarrow \quad 1 \equiv 16 \cdot 28 \mod 149$

ie. $28^{-1} \equiv 16 \mod 149$.

Hence:

$$28x \equiv 3 \mod 149$$

$\Leftrightarrow \quad x \equiv 28^{-1} \cdot 3 \mod 149$

$\equiv 16 \cdot 3 \mod 149$

$\Leftrightarrow \quad \boxed{x \equiv 48 \mod 149}$

5. [12 points] Suppose that a, b, c are positive integers such that $\gcd(a, b) = 1$. Prove that if a divides bc, then a divides c.

<u>Sol'n 1</u> (equation)

Since $\gcd(a,b)=1$, $\exists u,v \in \mathbb{Z}$ s.t.

$$au+bv=1.$$

Multiplying by c, we have:

$$cau + cbv = c$$

$$\Rightarrow a \cdot cu + a \cdot \frac{bc}{a} \cdot v = c$$

$$\Rightarrow a \cdot \left[cu + \frac{bc}{a} \cdot v\right] = c.$$

Since $a | bc$, $\frac{bc}{a} \in \mathbb{Z}$ so $cu + \frac{bc}{a} \cdot v \in \mathbb{Z}$ as well, & this shows that $\underline{a|c}$, as desired.

<u>Sol'n 2</u> (using congruences)

Since $a|bc$, we have

$$bc \equiv 0 \mod a.$$

Now, $\gcd(a,b)=1$ implies that $b^{-1} \mod a$ exists

so $$b^{-1} bc \equiv b^{-1} \cdot 0 \mod a$$

$$\Rightarrow c \equiv 0 \mod a$$

i.e. $a|c$ as well.

6. [12 points] Suppose that you enter a store carrying a large supply of 6 dollar coins. The shopkeeper is able to make change using 28 dollar coins and 63 dollar coins. Find a way that you can purchase a 1 dollar item.

For partial credit, you may first assume that both you and the shopkeeper have a large supply of all three types of coins (6,28, and 63) and solve the problem in this context.

We can solve $6u+28v+63w=0$ using two Euclids in a row:

$6u+28v$	u	v
28	0	1
6	1	0
$28-4\cdot 6=4$	-4	1
$6-4=2$	5	-1
$4-2\cdot 2=0$		

so $\gcd(6,28)=2$ & $2=5\cdot 6-1\cdot 28$.

Now, the euclidean algo. w/ 63, 2 has just one step:

$$63-31\cdot 2=1.$$

Plugging in the previous result,

$$\begin{aligned} 1 &= 63-31\cdot[5\cdot 6-1\cdot 28] \\ &= 63-155\cdot 6+31\cdot 28 \\ &= -155\cdot 6+31\cdot 28+1\cdot 63. \end{aligned}$$

So for the easier version of the problem, one solution is:

- you pay 31 \$28 coins & 1 \$63 coin.
- the shop gives you 155 \$6 coins in change.

To get a solution in the desired form, though, we can do the modification described in the linear equation theorem:

$$1 = 1\cdot 63 - 31\cdot 2$$

$$\Rightarrow 1 = (1-2)\cdot 63 + (-31+63)\cdot 2$$

$$= -1\cdot 63 + 32\cdot 2$$

is another sol'n w/ the signs we want.

It gives:

$$1 = -1\cdot 63 + 32\cdot[5\cdot 6 - 1\cdot 28]$$

$$= -1\cdot 63 + 160\cdot 6 - 32\cdot 28$$

$$= \underline{160\cdot 6 - 32\cdot 28 - 1\cdot 63}$$

so you can

- Pay 160 \$6 coins
- Get 32 \$28 coins & 1 \$63 coin in change.

(other solutions are also possible).