Math 471 Midterm 1 Spring 2019

Name: Solution

1. (10 points) Prove that any common divisor of two integers a and b is also a divisor of $\gcd(a, b)$. Hint: Recall that $\gcd(a, b)$ is a linear combination of a and b, by the Extended Euclidean Algorithm Theorem.

Assume that $d \mid a$ and $d \mid b$. Then $d \mid ax + by$, for all $x, y \in \mathbb{Z}$. Now, there exist $x, y \in \mathbb{Z}$, such that $\gcd(a,b) = ax + by$, by the E. E. A. Theorem. Hence $d \mid \gcd(a,b)$.

2. (12 points) Let a, b, n be positive integers. Prove that $\gcd(a^n, b^n) = \gcd(a, b)^n$.

Let $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ with p_i prime and $p_i \neq p_j$ if $i \neq j$, and $a_i \geq 0$ and $b_i \geq 0$.

Then $a^n = p_1^{na_1} \cdots p_k^{na_k}$ and

$b^n = p_1^{nb_1} \cdots p_k^{nb_k}$

$\gcd(a,b) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)}$ while

$\gcd(a^n, b^n) = p_1^{\min(na_1, nb_1)} \cdots p_k^{\min(na_k, nb_k)} =$

$= p_1^{n \cdot \min(a_1, b_1)} \cdots p_k^{n \cdot \min(a_k, b_k)} =$

$= \gcd(a, b)^n$.

Q.E.D

3. (15 points) Let $a = d_{99}d_{98}\cdots d_9d_8d_7d_6d_5d_4d_3d_2d_1d_0$ be the positive integer with 100 digits, where the digit d_i satisfies $0 \le d_i \le 9$ and $d_i \equiv i \pmod{10}$. So $a = 9876543210\cdots9876543210$.

(a) 5 pts Find the reduction of a modulo 9.

$$a \equiv \sum_{i=0}^{99} d_i = 10 \cdot \sum_{i=0}^{9} d_i \equiv (9+0)+(8+1)+(7+2)+(6+3)+(5+4) \equiv 0 \pmod 9$$

$10 \equiv 1 \pmod 9$

5 pts

(b) Find the reduction of a modulo 11.

$$a \equiv \sum_{i=0}^{99} (-1)^i d_i = 10 \cdot \sum_{i=0}^{9} (-1)^i d_i \equiv (-1)\left[(-9+8)+(-7+6)+(-5+4)+(-3+2)+(-1+0)\right]$$

$10 \equiv -1 \pmod{11}$

$= -5$

$$\equiv 5 \pmod{11}.$$

5 pt

(c) Use Parts 3a and 3b to find the reduction of a modulo 99. Carefully justify your answer.

We know that $a \equiv 0 \pmod 9$.

$a \equiv 5 \pmod{11}$.

If $t_0 \equiv 0 \pmod 9$ and $t_0 \equiv 5 \pmod{11}$, then $t_0 \equiv a \pmod{99}$. We find t_0 by solving $11x + 9y = 0 - 5$ and setting $t_0 = 11x + 5 = -9y$.

$11 \cdot x_i + 9 \cdot y_i = r_i$

x_i	y_i	r_i	q_i
1	0	11	–
0	1	9	–
1	-1	2	1
-4	5	1	4

$11(-4) + 9(5) = 1$

So $11(\underbrace{-4 \cdot (-5)}_{20}) + 9(5 \cdot (-5)) = -5$

$t_0 = 11 \cdot 20 + 5 = 225 \equiv 27$.

$\uparrow$ mod 99

So $\boxed{a \equiv 27 \pmod{99}}$.

7 pts

4. (15 points) Find the entire set of solutions for each of the systems of congruences. Express your answer as a single congruence. (a)

$$t \equiv 2 \pmod 3 \quad (1)$$
$$t \equiv 1 \pmod 5 \quad (2)$$

$\gcd(3,5) = 1$,

$11 \equiv 2 \pmod 3$

$11 \equiv 1 \pmod 5$,

So $t \equiv 11 \pmod{3 \cdot 5}$, by the Chinese Remainder Theorem.

$3 \cdot 5 = 15$

8 pts

(b) Use Part 4a to solve the following system of congruences.

$$t \equiv 2 \pmod 3 \quad (3)$$
$$t \equiv 1 \pmod 5 \quad (4)$$
$$t \equiv 0 \pmod 7 \quad (5)$$

(*) $\begin{cases} t \equiv 11 \pmod{15} \\ t \equiv 0 \pmod 7 \end{cases}$

Solve $15x + 7y = 0 - 11$. If (x_0, y_0) is a sol'n, then $t_0 = 15x + 11 = -7y$ is a solution of (*).

$15x_i + 7y_i = r_i$

x_i	y_i	r_i	q_i
1	0	15	–
0	1	7	–
1	−2	1	2

So $15(1) + 7(-2) = 1$

So $15(-11) + 7(22) = -11$

So $t_0 = 15 \cdot (-11) + 11 = -154 \equiv 56 \pmod{3 \cdot 5 \cdot 7}$

$3 \cdot 5 \cdot 7 = 105$

5. (12 points) The natural numbers a, b satisfy $\gcd(a,b) = 2$ and $\operatorname{lcm}(a,b) = 600$. Find all possible pairs of natural numbers satisfying these conditions.

a| $\operatorname{lcm}(a,b) = 2^3 \cdot 3 \cdot 5^2$ and $2 = \gcd(a,b) | a$ $\quad 2^3 \cdot 3 \cdot 5^2$

So $a = 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$ where

$1 \le a_1 \le 3, \quad 0 \le a_2 \le 1, \quad 0 \le a_3 \le 2$

Similarly $b = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3}$ where

$1 \le b_1 \le 3, \quad 0 \le b_2 \le 1, \quad 0 \le b_3 \le 2,$

Finally $2^{\min(a_1,b_1)} \cdot 3^{\min(a_2,b_2)} \cdot 5^{\min(a_3,b_3)} = 2^1 \cdot 3^0 \cdot 5^0$

$2^{\max(a_1,b_1)} \cdot 3^{\max(a_2,b_2)} \cdot 5^{\max(a_3,b_3)} = 2^3 \cdot 3^1 \cdot 5^2$

So $\boxed{\begin{array}{l} \min(a_1,b_1) = 1, \quad \min(a_2,b_2) = 0, \quad \min(a_3,b_3) = 0 \\ \max(a_1,b_1) = 3, \quad \max(a_2,b_2) = 1, \quad \max(a_3,b_3) = 2. \end{array}}$

$(a_1,b_1) \in \{(1,3) \text{ or } (3,1)\} \quad (a_2,b_2) \in \{(0,1) \text{ or } (1,0)\} \quad (a_3,b_3) \in \{(0,2),(2,0)\}$

8 - possibilities: First 4:

$(a,b) = (\underbrace{2^1 \cdot 3^0 \cdot 5^0}_{2}, \underbrace{2^3 \cdot 3^1 \cdot 5^2}_{600}), \quad (a,b) = (\underbrace{2^1 \cdot 3^1 \cdot 5^0}_{6}, \underbrace{2^3 \cdot 3^0 \cdot 5^2}_{200})$

$(a,b) = (\underbrace{2^1 \cdot 3^1 \cdot 5^2}_{150}, \underbrace{2^3 \cdot 3^0 \cdot 5^0}_{8}), \quad (a,b) = (\underbrace{2^1 \cdot 3^0 \cdot 5^2}_{50}, \underbrace{2^3 \cdot 3^1 \cdot 5^0}_{24})$

Another 4 are obtained by reversing the order in the right hand side of each of the 4 expressions above

6. (12 points) Let a, b be integers, not both zero. Set $d := \gcd(a, b)$. Prove that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Hint: Same as the hint for Problem 1.

By the Extended Euclidean Algorithm Theorem, there exist $x, y \in \mathbb{Z}$, such that $ax + by = d$. Dividing both sides by d we get

$$\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1$$

and $\frac{a}{d} \in \mathbb{Z}$, $\frac{b}{d} \in \mathbb{Z}$, since d is a common divisor. Let $c \in \mathbb{N}$ be a common divisor of $\frac{a}{d}, \frac{b}{d}$. Then c divides every linear combination of $\frac{a}{d}, \frac{b}{d}$ with integer coefficients. Hence, $c \mid 1$. Hence $c = 1$. Thus, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

7. (15 points)

(a) (5 pt) Use the Extended Euclidean Algorithm to find the general solution of the Diophantine equation $23x + 20y = 1$ (with x, y integers).

$23x_i + 20y_i = r_i$

x_i	y_i	r_i	q_i
1	0	23	–
0	1	20	–
1	-1	3	1
-6	7	2	6
7	-8	1	1

$23 \cdot 7 + 20(-8) = 1$

So the general sol'n is

$\{(7 - 20k, -8 + 23k) : k \in \mathbb{Z}\}$

(5 pt) (b) Find the general solution of the Diophantine equation $23x + 20y = 501$.

$501 \cdot (7, -8) = (3507, -4008)$ is a solution

The general sol'n is

$\{(3507 - 20k, -4008 + 23k) : k \in \mathbb{Z}\}$

(5 pt) (c) Find all solutions to the Diophantine equation in Part 7b with both x and y positive integers.

$3501 - 20k > 0 \iff k < \frac{3507}{20} = 175.35$

$-4008 + 23k > 0 \iff k > \frac{4008}{23} = 174.26\ldots$

So, $k = 175$ and the unique such solution is.

$(x, y) = (3507 - 20 \cdot 175, -4008 + 23 \cdot 175) = (7, 17)$

8. (12 points)

(a) For which integers a does the Diophantine equation $ax + (a+7)y = 1$ has a solution (with x, y integers)? Justify your answer!

(*)

$\gcd(a, a+7) = \gcd(a, (a+7)-a) = \gcd(a, 7)$.

↑ Euclid's Lemma.

Now $\gcd(a,7) \mid 1$ is a necessary and sufficient condition for the existence of a solution to (*),

so $\gcd(a,7) = 1$ (or equivalently $7 \nmid a$).

(*) has a solution $\Leftrightarrow 7 \nmid a$.

(b) Let a be a positive integer such that $a \equiv 1 \pmod 3$. Express the general solution of the Diophantine equation $ax + (a+3)y = 1$ in terms of a. Hint: Write $a = 3q + 1$.

$(3q+1)x + (3q+4)y = 1$

$(3q+4)y_i + (3q+1)x_i = r_i$

y_i	x_i	r_i	q_i
1	0	$3q+4$	—
0	1	$3q+1$	—
1	-1	3	1
$-q$	$q+1$	1	q

$(3q+1)(q+1) + (3q+4)(-q) = 1$

$3q^2+4q+1$ $\qquad -3q^2-4q$

$q = \frac{a-1}{3}$

General sol'n:

$\{(x,y) = (q+1-(a+3)k, -q+ak) : k \in \mathbb{Z}\}$

$\left\{(x,y) = \left(\frac{a+2}{3} - (a+3)k, \frac{1-a}{3} + ak\right) : k \in \mathbb{Z}\right\}$.