Homework 9

MATH 115
UC Berkeley
Guilherme Gomes Haetinger

November 10, 2019

4.5

1) Given any m integers none of which is a multiple of m, prove that two can be selected whose difference is a multiple of m.

Considering that, out of the m integers that aren't multiple to m, two of them must be of the same $\mod m$, we say that

$$x \equiv n \mod m \tag{1}$$
$$y \equiv n \mod m \tag{2}$$

This happens because of the *pigeonhole* principle, since there are only $m-1$ residue possibilities different than 0 and m integers that should fit in them. This way, we know that one residue must repeat and, concluding, from (1) and (2), $x - y = mk + n - (mw + n) = mk - mw = m(k - w)$, which is a multiple of m.

2) If S is any set of $n+1$ integers selected from $1, 2, 3, \cdot \cdot \cdot, 2n+1$, prove that S contains two relatively prime integers. Prove that the result does not hold if S contains only n integers.

Considering that two subsequent numbers are always relatively prime to each other, we know that, if you take $n-1$ numbers out of a set of $2n+1$ numbers, we know that there will be at least 2 numbers in sequence, i.e. co-prime. This happens due to the pigeonhole principle, which, in this case, for it to not have any subsequent numbers, we have $\frac{2n+1}{2}$ holes and $n+1$ entries. Since $n+1 > \frac{2n+1}{2}$, one of the numbers must be placed in a subsequent position.

The same thing explains why this doesn't happen when we pick n numbers, because $n < \frac{2n+1}{2}$.

5) Given any integers a, b, c and any prime p not a divisor of ab, prove that $ax^2 + by^2 \equiv c \mod p$ is solvable.

If p is even, $p = 2$. This way, we will always have solutions for $x^2 + y^2 \equiv c \mod 2$, c being either *0* or *1*.

If p is odd, we know that there are $\frac{p-1}{2}$ quadratic residues *modulus* p. Considering that $(a, p) = 1$, we know that ax^2 ranges from $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ residues *modulus* p. Similarly, we have the same for by^2 and to $c - by^2$. Therefore, we need $\exists x_0, y_0 \rightarrow a{x_0}^2 \equiv c - b{y_0}^2 \mod p$, otherwise we would have $2 * \frac{p+1}{2} = p + 1 > p$, which contradicts the fact that p has $p-1$ possible residues.

15) Let n be a positive integer having exactly three distinct prime factors p, q and r. Find a formula for the number of positive integers $\leq n$ that are divisible by none of pq, pr, or qr.

This is a set problem. We have the sets of numbers that are divisible by p, q and r, we have the set of numbers that are less or equal to n and we want to find the the sets of numbers that aren't divisible by any permutation of these. For that, we have

$$S = \{x, x \leq n\} \tag{3}$$
$$P = \{x, x \in S, p|x\} \tag{4}$$
$$Q = \{x, x \in S, q|x\} \tag{5}$$
$$R = \{x, x \in S, r|x\} \tag{6}$$
$$x = S - (P \cap Q) - (P \cap R) - (Q \cap R) + 2 * (P \cap Q \cap R) \tag{7}$$

We have to subtract from the greater set the intersection between the multiples of each prime and then add 2 times the intersection of all the three primes, since it's being subtracted 3 times and we only want it to be once.

5.1

4 Find the solutions in positive integers for

- $5x + 3y = 52$

$$\begin{array}{ccc} 5 & 3 & 52 \\ \hline 1 & 0 & \\ 0 & 1 & \end{array} \rightarrow \begin{array}{ccc} 2 & 3 & 52 \\ \hline 1 & 0 & \\ -1 & 1 & \end{array} \rightarrow \begin{array}{ccc} 2 & 1 & 52 \\ \hline 1 & -1 & \\ -1 & 2 & \end{array} \rightarrow \begin{array}{ccc} 0 & 1 & 52 \\ \hline 3 & -1 & \\ -5 & 2 & \end{array}$$

$$v = 52 \tag{1}$$
$$x = 3u - v = 3u - 52 \tag{2}$$
$$y = -5u + 2v = -5u + 104 \tag{3}$$
$$u = t + 17 \tag{4}$$
$$x = 3t - 1 \tag{5}$$
$$y = -5t + 19 \tag{6}$$

- $15x + 7y = 111$

$$\begin{array}{ccc} 15 & 7 & 111 \\ \hline 1 & 0 & \\ 0 & 1 & \end{array} \rightarrow \begin{array}{ccc} 1 & 7 & 111 \\ \hline 1 & 0 & \\ -2 & 1 & \end{array} \rightarrow \begin{array}{ccc} 1 & 0 & 111 \\ \hline 1 & -7 & \\ -2 & 15 & \end{array}$$

$$u = 111 \tag{1}$$
$$x = u - 7v = 111 - 7v \tag{2}$$
$$y = -2u + 15v = -222 + 15v \tag{3}$$
$$v = t + 14 \tag{4}$$
$$x = 13 - 7t \tag{5}$$
$$y = 15t - 12 \tag{6}$$

- $12x + 50y = 1$

$$\begin{array}{ccc} 12 & 50 & 1 \\ \hline 1 & 0 & \\ 0 & 1 & \end{array} \rightarrow \begin{array}{ccc} 12 & 2 & 1 \\ \hline 1 & -4 & \\ 0 & 1 & \end{array} \rightarrow \begin{array}{ccc} 0 & 2 & 1 \\ \hline 25 & -4 & \\ -6 & 1 & \end{array}$$

$$v = 0.5 \quad (1)$$
$$x = 25u - 4v = 25u - 2 \quad (2)$$
$$y = -6u + v = -6u + 0.5 \quad (3)$$

- $97x + 98y = 1000$

97	98	1000		97	1	1000		0	1	1000
1	0		$\rightarrow$	1	-1		$\rightarrow$	98	-1	
0	1			0	1			-97	1	

$$v = 1000 \quad (1)$$
$$x = 98u - v = 98u - 1000 \quad (2)$$
$$y = -97u + v = -97u + 1000 \quad (3)$$
$$u = t + 10 \quad (4)$$
$$x = 98t - 20 \quad (5)$$
$$y = -97t + 30 \quad (6)$$

8) If $ax + by = c$ is solvable, prove that it has a solution x_0, y_0 with $0 \leq x_0 < |b|$.

We know, by *Theorem 5.1*, that all solutions are of the form $\{x_0 + k\frac{b}{g}, y_0 - k\frac{a}{g}\}$. Thus we can say that, because $|\frac{b}{g}| \leq |b|$, there is such a x_0.

16) Let a and b be positive integers with $g.c.d.(a, b) = 1$. Let S denote the set of all integers that may be expressed in the form $ax + by$ where x and y are non-negative integers. Show that $c = ab - a - b$ is not a member of S, but that every integer larger than c is a member of S.

Knowing that $ax + by = c = ab - a - c$, we can express $x_0 = -1, y_0 = a - 1$, making, in this case, all solutions represented by $\{kb - 1, a - 1 - ka\}$. Thus, c will never have positive coefficients, whichever side k grows to.

Let $d > c = ab - a - b \rightarrow d \geq ab - a - b + 1$. By question #8, we know that there is a solution to $ax + by = d$ with $0 \leq x_0 < b \rightarrow 0 \leq x_0 \leq b - 1$. We want to show that there is a $y_0 \geq 0$.

$$0 \leq x_0 \leq b - 1 \quad (1)$$
$$0 \leq ax_0 \leq ab - a \quad (2)$$
$$\tfrac{d-(ab-a)}{b} \leq \tfrac{d-ax_0}{b} \leq \tfrac{d}{b} \quad (3)$$
$$\tfrac{d-(ab-a)}{b} \geq \tfrac{(ab-a-b+1)-(ab-a)}{b} = \tfrac{-b+1}{b} = -1 + \tfrac{1}{b} > -1 \quad (4)$$

We can see that the second element of the inequality (3) is equal to y_0. Thus we know that $y_0 > -1$ and, since $y_0 \in \mathbb{Z}$, we know that $y_0 \geq 0$ and, hence, that d is a part of S.

5.2

1) Find all solutions in integers of the system of equations

$$x_1 + x_2 + 4x_3 + 2x_4 = 5$$
$$-3x_1 - x_2 - 6x_4 = 3$$
$$-x_1 - x_2 + 2x_3 - 2x_4 = 1$$

$$
\begin{array}{rrrrr}
1 & 1 & 4 & 2 & 5 \\
-3 & -1 & 0 & -6 & 3 \\
-1 & -1 & 2 & -2 & 1 \\
\hline
1 & 0 & 0 & 0 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrrr}
1 & 0 & 0 & 0 & 5 \\
-3 & 2 & 12 & 0 & 3 \\
-1 & 0 & 6 & 0 & 1 \\
\hline
1 & -1 & -4 & -2 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrrr}
1 & 0 & 0 & 0 & 5 \\
-3 & 2 & 12 & 0 & 3 \\
0 & 0 & 6 & 0 & 6 \\
\hline
1 & -1 & -4 & -2 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
$$

$$
\begin{array}{rrrrr}
1 & 0 & 0 & 0 & 5 \\
0 & 0 & 6 & 0 & 6 \\
-2 & 2 & 12 & 0 & 8 \\
\hline
1 & -1 & -4 & -2 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrrr}
1 & 0 & 0 & 0 & 5 \\
0 & 2 & 0 & 0 & 8 \\
0 & 0 & 6 & 0 & 6 \\
\hline
0 & -1 & 2 & -2 & \\
1 & 1 & -6 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
$$

Now we have:

$$
\begin{aligned}
u = & \quad 5 \\
2v = 8 \rightarrow v = & \quad 4 \\
6w = 6 \rightarrow w = & \quad 1 \\
x_1 = & \quad -v + 2w - 2t = -2 - 2t \\
x_2 = & \quad u + v - 6w = 3 \\
x_3 = & \quad w = 1 \\
x_4 = & \quad t
\end{aligned}
$$

2) For what integers *a*, *b* and *c* does the system of equations

$$
\begin{aligned}
x_1 + 2x_2 + 3x_3 + 4x_4 =& a \\
x_1 + 4x_2 + 9x_3 + 16x_4 =& b \\
x_1 + 8x_2 + 27x_3 + 64x_4 =& c
\end{aligned}
$$

$$
\begin{array}{rrrrl}
1 & 2 & 3 & 4 & \text{a} \\
1 & 4 & 9 & 16 & \text{b} \\
1 & 8 & 27 & 64 & \text{c} \\
\hline
1 & 0 & 0 & 0 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrrl}
1 & 0 & 0 & 0 & \text{a} \\
1 & 2 & 6 & 12 & \text{b} \\
1 & 6 & 24 & 60 & \text{c} \\
\hline
1 & -2 & -3 & -4 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrrl}
1 & 0 & 0 & 0 & \text{a} \\
0 & 2 & 6 & 12 & \text{b-a} \\
0 & 6 & 24 & 60 & \text{c-a} \\
\hline
1 & -2 & -3 & -4 & \\
0 & 1 & 0 & 0 & \\
0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 1 &
\end{array}
$$

$$
\begin{array}{rrrl}
2 & 6 & 12 & \text{b-a} \\
6 & 24 & 60 & \text{c-a} \\
\hline
-2 & -3 & -4 & \\
1 & 0 & 0 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrl}
2 & 0 & 0 & \text{b-a} \\
6 & 6 & 24 & \text{c-a} \\
\hline
-2 & 3 & 8 & \\
1 & -3 & -6 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrrl}
2 & 0 & 0 & \text{b-a} \\
0 & 6 & 24 & \text{c+2a-b} \\
\hline
-2 & 3 & 8 & \\
1 & -3 & -6 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
$$

$$
\begin{array}{rrl}
6 & 24 & \text{c+2a-b} \\
\hline
3 & 8 & \\
-3 & -6 & \\
1 & 0 & \\
0 & 1 &
\end{array}
\rightarrow
\begin{array}{rrl}
6 & 0 & \text{c+2a-b} \\
\hline
3 & -4 & \\
-3 & 6 & \\
1 & -4 & \\
0 & 1 &
\end{array}
$$

Which leaves us with the following:

$$\begin{aligned}
u =& a \\
v =& \frac{b-a}{2} \\
w =& \frac{c+2a-b}{6} \\
x_1 =& u - 2v + 3w - 4t \\
x_2 =& v - 3w + 6t \\
x_3 =& w - 4t \\
x_4 =& t
\end{aligned}$$

When $a = b = c = 1$, we have the following values:

$$\begin{aligned}
x_1 =& 1 - 4t \\
x_2 =& 6t \\
x_3 =& -4t \\
x_4 =& t
\end{aligned}$$