CS 70 Discrete Mathematics and Probability Theory
Fall 2017 Satish Rao and Kannan Ramchandran

HW 4

Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up. (*signature here*)

1 Don't Try This at Home

A ticket in the lottery consists of six numbers chosen from $1, 2, \ldots, 48$ (repetitions allowed). After everyone has bought their tickets, the manager picks 5 winning numbers from this set at random. Your ticket wins if it contains each of these winning numbers. Order is irrelevant.

Prove that if you buy all possible tickets for which the sum of the six entries on the ticket is divisible by 47, then you are guaranteed to have a winner.

Solution:

We show that, for any choice of the winning numbers, there exists a winning ticket whose sum of entries is divisible by 47.

Let a, b, c, d, e be the winning numbers, and let $s = -a - b - c - d - e \mod 47$.

(Let's assume that we take s to be the smallest positive integer satisfying this congruence modulo 47.) Then consider the ticket a, b, c, d, e, s. This is a valid ticket, since $1 \leq s \leq 47$. It is a winning ticket, since it contains the winning numbers a, b, c, d, e. Finally, it is a ticket we would have bought, since we have $a + b + c + d + e + s \equiv 0 \pmod{47}$, and thus the sum of entries on this ticket is a multiple of 47.

2 Euclid's Algorithm

(a) Use Euclid's algorithm from lecture to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.

(b) Use extended Euclid's algorithm from lecture to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.

(c) Find $x \pmod{27}$ if $5x + 26 \equiv 3 \pmod{27}$. You can use the result computed in (b).

(d) Assume a, b, and c are integers and $c > 0$. Prove or disprove: If a has no multiplicative inverse mod c, then $ax \equiv b \pmod{c}$ has no solution.

Solution:

(a) The values of x and y of all recursive calls are (you can get full credits without the column of x mod y):

Function Calls	(x, y)	x mod y
#1	$(527, 323)$	204
#2	$(323, 204)$	119
#3	$(204, 119)$	85
#4	$(119, 85)$	34
#5	$(85, 34)$	17
#6	$(34, 17)$	0
#7	$(17, 0)$	—

Therefore, $\gcd(527, 323) = 17$.

(b) To compute the multiplicative inverse of 5 mod 27, we first call `extended-gcd(27,5)`. Note that `(x div y)` in the pseudocode means $\lfloor x/y \rfloor$. The values of x and y of all recursive calls are (you can get full credits without the columns of x div y and x mod y):

Function Calls	(x, y)	x div y	x mod y
#1	$(27, 5)$	5	2
#2	$(5, 2)$	2	1
#3	$(2, 1)$	2	0
#4	$(1, 0)$	—	—

The returned values of all recursive calls are:

Function Calls	(d, a, b)	Returned Values
#4	—	$(1, 1, 0)$
#3	$(1, 1, 0)$	$(1, 0, 1)$
#2	$(1, 0, 1)$	$(1, 1, -2)$
#1	$(1, 1, -2)$	$(1, -2, 11)$

Therefore, we get $1 = (-2) \times 27 + 11 \times 5$ and

$$1 = (-2) \times 27 + 11 \times 5 \equiv 11 \times 5 \pmod{27},$$

so the multiplicative inverse of 5 mod 27 is 11.

(c)

$$\begin{aligned} 5x + 26 \equiv 3 \pmod{27} &\Rightarrow 5x \equiv 3 - 26 \pmod{27} \\ &\Rightarrow 5x \equiv -23 \pmod{27} \\ &\Rightarrow 5x \equiv 4 \pmod{27} \\ &\Rightarrow 11 \times 5x \equiv 11 \times 4 \pmod{27} \\ &\Rightarrow x \equiv 44 \pmod{27} \\ &\Rightarrow x \equiv 17 \pmod{27}. \end{aligned}$$

(d) False. We can have a counterexample: $a = 3$, $b = 6$, and $c = 12$, so a has no multiplicative inverse mod c (because $a = 3$ and $c = 12$ are not relatively prime). However, $3x \equiv 6 \pmod{12}$ has solutions $x = 2, 6, 10 \bmod 12$.

3 Solution for $ax \equiv b \pmod{m}$

In the notes, we proved that when $\gcd(m, a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \pmod{m}$ has exactly one solution x (modulo m). This proof also implies that when $\gcd(m, a) = 1$, there is a unique solution to $ax \equiv b \pmod{m}$, where x is the unknown variable.

Now consider the equation $ax \equiv b \pmod{m}$, when $\gcd(m, a) > 1$.

(a) Let $\gcd(m, a) = d$. Prove that $ax \equiv b \pmod{m}$ has a solution (that is, there exists an x that satisfies this equation) if and only if $b \equiv 0 \pmod{d}$.

(b) Let $\gcd(m, a) = d$. Assume $b \equiv 0 \pmod{d}$. Prove that $ax \equiv b \pmod{m}$ has exactly d solutions (modulo m).

(c) Solve for x: $77x \equiv 35 \pmod{42}$.

Solution:

(a) **Necessary condition:** $ax \equiv b \pmod{m}$ has a solution $\implies b \equiv 0 \pmod{d}$.

If $ax \equiv b \pmod{m}$ has a solution, we can write $ax = my + b$ for some $x, y \in \mathbb{Z}$.
Since d is the greatest common divisor of m and a, we know that $d \mid a$ and $d \mid m$. Therefore d divides $ax - my = b$, or equivalently, $b \equiv 0 \pmod{d}$.

Sufficient condition: $b \equiv 0 \pmod{d} \implies ax \equiv b \pmod{m}$ has a solution.

Consider the congruent equation

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \tag{1}$$

We know that

$$\gcd(m,a) = d \implies \gcd\left(\frac{m}{d}, \frac{a}{d}\right) = 1.$$

Therefore (1) has a solution, or equivalently, $\exists x, y \in \mathbb{Z}$, such that

$$\frac{a}{d}x = \frac{m}{d}y + \frac{b}{d}.$$

$\implies ax = my + b.$
$\implies x$ is a solution for $ax \equiv b \pmod{m}$.

Alternate proof for sufficient condition:

If $d \mid b$, we can write $b = kd$ for some $k \in \mathbb{Z}$. Since $\gcd(m,a) = d$, $\exists w, y \in \mathbb{Z}$, such that $aw + my = d$, similar to what we've seen with extended Euclid's algorithm. Multiplying both sides by k, we get $kaw + kmy = kd = b$. So

$$akw + mky \equiv b \pmod{m},$$
$$akw \equiv b \pmod{m}.$$

Then, kw is a solution of $ax \equiv b \pmod{m}$.

(b) From the proof of sufficient condition in Part (a), we have shown that if x satisfies (1), then x also satisfies $ax \equiv b \pmod{m}$. How about the reverse?
If x satisfies $ax \equiv b \pmod{m}$, then

$$ax = my + b \text{ for some } y \in \mathbb{Z},$$
$$\implies \frac{a}{d}x = \frac{m}{d}y + \frac{b}{d},$$
$$\implies x \text{ satisfies } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

We conclude the following Lemma from the above proof:

Lemma: $\forall x \in \mathbb{Z}$, x satisfies (1) if and only if x satisfies $ax \equiv b \pmod{m}$.

Let x_0 be the unique solution of (1). Any $x \in \mathbb{Z}$ that satisfies (1) must be of the form

$$x = x_0 + k\frac{m}{d} \qquad \text{for some } k \in \mathbb{Z}. \tag{2}$$

By the above Lemma, any $x \in \mathbb{Z}$ that satisfies $ax \equiv b \pmod{m}$ will also be of the form (2).

Now we will show that there are only d distinct solutions (modulo m) for $ax \equiv b \pmod{m}$ of the form (2). Two solutions,

$$x_1 = x_0 + k_1\frac{m}{d}$$
$$x_2 = x_0 + k_2\frac{m}{d}$$

are the same in modulo m if and only if

$$\begin{aligned} x_0 + k_1\frac{m}{d} \equiv x_0 + k_2\frac{m}{d} \pmod{m} &\iff (k_1-k_2)\frac{m}{d} \equiv 0 \pmod{m}, \\ &\iff (k_1-k_2)\frac{m}{d} = qm \text{ for some } q \in \mathbb{Z}, \\ &\iff (k_1-k_2)m = qmd, \\ &\iff k_1 - k_2 = qd. \end{aligned}$$

The above argument proved that two solutions with the form (2) are equal $\pmod{m}$ if and only if $k_1 \equiv k_2 \pmod{d}$. Without loss of generality, we can construct solutions by letting $k \in \{0, 1, \ldots, d-1\}$. To be very specific, the d distinct solutions of $ax \equiv b \pmod{m}$ are

$$x \equiv x_0 + k\frac{m}{d} \pmod{m}, \qquad k = 0, 1, \ldots, d-1.$$

(c) Since $\gcd(77, 42) = 7$ and $35 \equiv 0 \pmod{7}$, we can find a unique solution from $(77/7)x \equiv 35/7 \pmod{42/7}$:

$$\begin{aligned} 11x &\equiv 5 \pmod{6} \\ -1x &\equiv -1 \pmod{6} \qquad (\text{because } 11 \equiv -1 \pmod{6} \text{ and } 5 \equiv -1 \pmod{6}) \\ x &\equiv 1 \pmod{6} \end{aligned}$$

The solution of $(77/7)x \equiv 35/7 \pmod{42/7}$ is $x \equiv 1 \pmod{6}$. Based on Part (b), the solutions of $77x \equiv 35 \pmod{42}$ are

$$x \equiv 1 + 6k \pmod{42}, \qquad k = 0, 1, \ldots, 6.$$

4 Nontrivial Modular Solutions

(a) What are all the possible squares modulo 4? Show that any solution to $a^2 + b^2 \equiv 3c^2 \pmod{4}$ must satisfy $a^2 \equiv b^2 \equiv c^2 \equiv 0 \pmod{4}$.

(b) Using part (a), prove that $a^2 + b^2 = 3c^2$ has no non-trivial solutions (a, b, c) in the integers. In other words, there are no integers a, b, and c that satisfy this equation, except the trivial solution $a = b = c = 0$.

[*Hint:* Consider some nontrivial solution (a, b, c) with the smallest positive value for a (why are we allowed to consider this?). Then arrive at a contradiction by finding another solution (a', b', c') with $a' < a$.]

Solution:

(a) Checking by hand, the only squares modulo 4 are 0 and 1 (for example, $3^2 \equiv 1 \pmod 4$). Considering the equation $a^2 + b^2 \equiv 3c^2 \pmod 4$, this means that $a^2 + b^2 \pmod 4$ can only be one of the following: 0, 1, 2.

None of these possibilities is consistent with $c^2 \equiv 1 \pmod 4$, so we must have $c^2 \equiv 0 \pmod 4$. This forces $a^2 \equiv b^2 \equiv 0 \pmod 4$, so a^2, b^2, c^2 are all divisible by 4.

(b) Notice that if (a,b,c) is a solution to $a^2 + b^2 = 3c^2$, then $(-a,b,c)$ is also a solution. Let's assume that some nontrivial solution exists, and (a,b,c) is the solution with the smallest positive value of a. This "smallest" solution must exist by the well-ordering principle. It's not meaningful to consider the solution with the smallest overall value of a because of our first observation that $-a$ is also part of another solution.

If (a,b,c) is a solution to the original equation, then this is also a solution to

$$a^2 + b^2 \equiv 3c^2 \pmod 4.$$

From Part (a), we know that a^2, b^2, c^2 are all divisible by 4, which in turn means that a, b, c are all divisible by 2. If we divide the entire original equation by 4, we see that

$$\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = 3\left(\frac{c}{2}\right)^2.$$

Indeed, $(a/2, b/2, c/2)$ is another solution with a smaller positive value of a where all the values are integers. We've reached a contradiction to our initial assumption, which was that (a,b,c) was the solution with the least positive value of a. Thus, there does not exist a nontrivial solution to $a^2 + b^2 = 3c^2$.