

DISCRETE MATH, HOMEWORK 11 SOLUTIONS

1. There are a number of ways to organize the arithmetic here, but the one closest to what we did in class is to start out by computing $\gcd(2013, 902) = 11$ using Euclid's algorithm. If you divide the whole equation by 11, you get

$$(1) \quad 183x - 82y = 6.$$

Now we try our Euclid's algorithm approach to this. We get

$$183 = 82 \cdot 2 + 19$$

$$82 = 19 \cdot 4 + 6$$

$$19 = 6 \cdot 3 + 1.$$

Next, we find an initial solution to $183x - 82y = 1$ by writing equations for the remainders and substituting, as always:

$$19 = 183 - 82 \cdot 2$$

$$6 = 82 - 19 \cdot 4$$

$$1 = 19 - 6 \cdot 3;$$

so

$$1 = 19 - [82 - 19 \cdot 4]3 = 19(13) - 82(3)$$

$$1 = [183 - 82 \cdot 2](13) - 82(3) = 183(13) - 82(29).$$

Multiplying by 6 gives us the initial solution

$$183(78) - 82(174) = 6$$

for equation (1)

Given this first solution, we know what all the solutions will look like:

$$x = 78 + 82t$$

$$y = 174 + 183t,$$

where t ranges over all integers. We need to show that all these points are solutions to our equation, and that there can be no other solutions.

That all these points are solutions is easy: just plug them into equation (1), and you get

$$\begin{aligned} 183(78 + 82t) - 82(174 + 183t) &= 183(78) + 183(82t) - 82(174) - 82(183t) \\ &= 183(78) - 82(174) = 6. \end{aligned}$$

To show that there could be no other solutions, suppose (x, y) is any solution. Then we have

$$183x - 82y = 6$$

$$183(78) - 82(174) = 6.$$

Subtracting, we get

$$183(x - 78) - 82(y - 174) = 0,$$

or

$$183(x - 78) = 82(y - 174).$$

This means that $82 \mid (183(x - 78))$. Since $\gcd(82, 183) = 1$, the Fundamental Theorem of Arithmetic says that $82 \mid (x - 78)$, i.e., that $x - 78 = 82t$ for some integer t . Rearranging, we have $x = 78 + 82t$, as desired. Plugging this into the previous equation, we get

$$82(y - 174) = 183(x - 78) = 183(82t),$$

so that $y - 174 = 183t$, and $y = 174 + 183t$. Every solution is therefore of the form we claimed, and we are done.

- 2. (a)** The two congruences can be turned into equations saying

$$\begin{aligned} x &= 28 + 45u \\ x &= 113 + 400v. \end{aligned}$$

This means that $28 + 45u = 113 + 400v$; or that $45u - 400v = 85$.

This Diophantine equation can be solved just like always. We first divide everything in sight by 5 to turn the equation into $9u - 80v = 17$. We then solve $9u - 80v = 1$; just looking at the equation gives us the initial solution

$$9(9) - 80(1) = 1.$$

Now multiply by 17 to get $9(153) - 80(17) = 17$.

The same reasoning as in Problem 1 shows that the general solution to the Diophantine equation is therefore

$$\begin{aligned} u &= 153 + 80t, \\ v &= 17 + 9t. \end{aligned}$$

Plugging either of these expressions into our original equation gives

$$x = 28 + 45u = 28 + 45(153 + 80t) = 6913 + 3600t,$$

so that

$$x \equiv 6913 \equiv 3313 \pmod{3600}.$$

- (b)** This time, the congruences reduce to

$$\begin{aligned} 20 + 45u &= 112 + 400v \\ 45u - 400v &= 92. \end{aligned}$$

This equation plainly has no solutions in \mathbb{Z} , since $5 \mid (45u - 400v)$, but $5 \nmid 92$.

- 3.** The base case at $n = 0$ says that

$$4 \cdot 5^0 = 5^1 - 1,$$

which is true by inspection.

Suppose, then, that for some fixed n ,

$$4(5^0) + 4(5^1) + \cdots + 4(5^n) = 5^{n+1} - 1.$$

We want to show that

$$4(5^0) + 4(5^1) + \cdots + 4(5^n) + 4(5^{n+1}) = 5^{n+2} - 1.$$

By the induction hypothesis,

$$\begin{aligned} 4(5^0) + 4(5^1) + \cdots + 4(5^n) + 4(5^{n+1}) &= (5^{n+1} - 1) + 4(5^{n+1}) \\ &= 5(5^{n+1}) - 1 \\ &= 5^{n+2} - 1. \end{aligned}$$

The result follows by induction.

4. One could do this in a number of ways, but here is one that mimics our proof for $\sqrt{2}$ as closely as possible. Suppose $\sqrt{1/5}$ were rational. Then one could write

$$\sqrt{1/5} = \frac{a}{b},$$

where a and b are integers and $\gcd(a, b) = 1$. Thus

$$\begin{aligned} \frac{1}{5} &= \frac{a^2}{b^2} \\ b^2 &= 5a^2. \end{aligned}$$

This tells us that $5 \mid b^2$, from which we infer that $5 \mid b$. Why? Our quick argument at this point says we have $5 \mid b \cdot b$. If $5 \mid b$, we are done. If $5 \nmid b$, then $\gcd(5, b) = 1$ (since 5 and 1 are the only positive divisors of 5). By the Fundamental Theorem of Arithmetic, it follows that $5 \mid b$, and we are also done.

Now we can write $b = 5\beta$, where $\beta \in \mathbb{Z}$. Thus,

$$\begin{aligned} 5a^2 &= b^2 = (5\beta)^2 \\ a^2 &= 5\beta^2. \end{aligned}$$

This means that $5 \mid a^2$; so by the same reasoning as before, $5 \mid a$. But this is a contradiction: it can't be the case that $\gcd(a, b) = 1$ if both a and b are multiples of 5. Therefore our initial hypothesis must be wrong: $\sqrt{1/5}$ must be irrational.

One could instead have proved that $\sqrt{5}$ is irrational. This would force $\sqrt{1/5} = 1/\sqrt{5}$ to be irrational; since if $\sqrt{1/5} = a/b$ were rational, then so would be $\sqrt{5} = b/a$.

5. It's false. For instance, in \mathbb{Z}_{10} . $4 \cdot 2 = 4 \cdot 7$, but $2 \neq 7$.

A possible salvage would be that if p is a prime and if $ac = bc$ and $c \neq 0$ in \mathbb{Z}_p , then $a = b$ in \mathbb{Z}_p . The proof says that if $ac = bc$ and $c \neq 0$, then $\gcd(c, p) = 1$; so that $\frac{1}{c}$ exists in \mathbb{Z}_p . Multiplying by $\frac{1}{c}$ gives

$$a = ac \frac{1}{c} = bc \frac{1}{c} = b,$$

as desired.

6. (a) For no particular reason, let's try starting with $a = 2$. Then

$$\begin{aligned} 2^2 &= 4 \\ 2^4 &= (2^2)^2 = 4^2 = 16 \\ 2^8 &= (2^4)^2 = 16^2 = 256 = 123 = -10 \\ 2^{16} &= (2^8)^2 = (-10)^2 = 100 = -33 \\ 2^{32} &= (2^{16})^2 = (-33)^2 = 1089 = 25 \\ 2^{64} &= (2^{32})^2 = (25)^2 = 625 = 93 = -40 \\ 2^{128} &= (2^{64})^2 = (-40)^2 = 1600 = 4. \end{aligned}$$

Notice that we never have to deal with numbers of more than 4 digits.

Thus,

$$2^{132} = 2^{128}2^4 = 4 \cdot 16 = 64 \neq 1;$$

so 133 is not a prime.

- (b) I would have accepted either of the following answers:

No, because every time you apply Fermat's Test, you will find that $a^{58} = 1$, which tells you that 59 might or might not be prime.

Yes. Apply Fermat's Test to every single $a \neq 0$ in \mathbb{Z}_{59} . You'll get $a^{58} = 1$ every single time. If 59 were composite, then one of these numbers a would have to be a divisor of 59. This would mean that in \mathbb{Z}_{59} , we would have $a^{58} = a^{58} - 59y$, which would be a multiple of a . But we never got a multiple of any a ; we always got 1. Therefore 59 must be prime. In fact, it would have worked to use every a from 1 up to $\sqrt{59}$. See why? Of course, this is a completely useless way to prove primality, since it would be much quicker just to divide 59 by every number up to $\sqrt{59}$ and show that the quotient is never an integer.

7. (a) The number a is an identity element for addition ($a + x = x$ for all x), and $ax = a$ for all x in the arithmetic. On either ground (but especially on the first), a would seem like a good choice for 0.
- (b) Similarly, b is an identity element for multiplication ($bx = x$ for all x); so b would seem to be the right choice for 1.
- (c) $a + a = a = 0$; so $-a = a$. Also, $b + d = a = 0$; so $-b = d$ and $-d = b$. Similarly, $c + c = e + e = f + f = a = 0$, so $-c = c$, $-e = e$, and $-f = f$. Finally, $g + h = a$; so $-g = h$ and $-h = g$.
- (d) Under multiplication, we've got $bb = b = 1$, which means $1/b = b$. Similarly, $dd = b = 1$; so $1/d = d$. Also, $gh = b = 1$; so $1/g = h$ and $1/h = g$. No other product gives you b ; so a , c , e , and f do not have multiplicative inverses.
- (e) Finally, it looks from the multiplication table as though $a^2 = c^2 = a$, which means that \sqrt{a} is either a or c . On the same grounds, \sqrt{b} is b or d ; \sqrt{c} is e or f ; and \sqrt{d} is g or h . No other element of this arithmetic has a square root.

If you're interested in where this system came from, it's a modular arithmetic obtained by starting with $\mathbb{Z}[i]$, the set of complex numbers whose real and imaginary parts are both integers. When you divide by $2 + i$ in this system, it is possible to arrange things so that every number leaves a remainder of either 0, 1, 2, 3, $1 + i$, $1 - i$, $2 + 1$, or $2 - i$. These remainders are the numbers a - h , resp. In other words, this arithmetic is $\mathbb{Z}[i]_{2+i}$.